

Google Cybersecurity Certificate



Key Competencies & Job Mapping

Developing talent for in-demand jobs

Prepare for a new career in the high-growth field of cybersecurity, no degree or experience required. Get professional training designed and delivered by subject matter experts at Google and have the opportunity to connect with top employers.

The Google Career Cybersecurity Certificate helps prepare you for the CompTIA Security+ exam, the industry leading certification for cybersecurity roles. You'll earn a dual credential when you complete both. The certificates can be completed in under three months part-time.

GOOGLE Cybersecurity CERTIFICATE

The Google Cybersecurity Certificate is designed to prepare learners for entry-level roles in Cybersecurity.

Additionally, each course includes portfolio activities through which you'll showcase examples of cybersecurity skills that you can share with potential employers. Acquire concrete skills that top employers are hiring for right now..

200K+

in-demand job openings
in Cybersecurity ¹

82%

of Google Career Certificate graduates say the program helped them advance their job search or career within three to six months ⁵

THE GOOGLE Cybersecurity CERTIFICATE PREPARES LEARNERS FOR IN-DEMAND JOBS SUCH AS:

- Cybersecurity analyst
- Associate Cybersecurity analyst
- Security analyst
- Security operations center (SOC) analyst

¹Lightcast™ US Job Postings (median salary with 0-5 years experience), Jan. 1, 2022 - Dec. 31, 2022).

²Positive career outcome (e.g., new job, promotion, or raise) within six months of completion. Based on program graduate survey, United States 2022.

Program overview

Upon completing the **Google Cybersecurity Certificate**, program graduates will:

- Understand the importance of cybersecurity practices and their impact for organizations.
- Protect networks, devices, people, and data from unauthorized access and cyberattacks using Security Information and Event Management (SIEM) tools.
- Identify common risks, threats, and vulnerabilities, as well as techniques to mitigate them.
- Gain hands-on experience with Python, Linux, and SQL.



Python Programming



Coding



Linux



Security Information and Event Management (SIEM) tools



Intrusion Detection Systems (IDS)



SQL

Course 1

Foundations of Cybersecurity

Course 2

Play It Safe: Manage Security Risks

Course 3

Connect and Protect: Networks and Network Security Data for Exploration

Course 4

Tools of the Trade: Linux and SQL

Course 5

Assets, Threats, and Vulnerabilities

Course 6

Sound the Alarm: Detection and Response

Course 7

Automate Cybersecurity Tasks with Python

Course 8

Put It to Work: Prepare for Cybersecurity Jobs

CONTENT BREAKDOWN:



297

Videos



223

Readings



136

Quizzes



86

Hands-on Exercises



40

Writing Assignments



41

Discussion Prompts

Course 1 — Foundations of Cybersecurity

In this course, we cover foundational Cybersecurity terminology and learners gain a deeper understanding of the role and responsibilities of a Cybersecurity analyst. We also introduce the kinds of jobs learners might pursue after completing this program.

By the end of this course, learners will be able to:

- Identify how security attacks impact business operations.
- Explore the job responsibilities and core skills of an entry-level cybersecurity analyst.
- Recognize how past and present attacks on organizations led to the development of the cybersecurity field.
- Learn the CISSP eight security domains.
- Identify security domains, frameworks, and controls.
- Explain security ethics.
- Recognize common tools used by cybersecurity analysts..






SKILLS ACQUIRED:

- ❑ Information Security (INFOSEC)
- ❑ Cybersecurity
- ❑ Historical Attacks
- ❑ Ethics in cybersecurity
- ❑ NIST Cybersecurity Framework (CSF)

TOPICS:

- ★ Introducing Cybersecurity
- ★ Thinking analytically
- ★ Exploring the wonderful world of data
- ★ Setting up a data toolbox
- ★ Discovering data career possibilities

CONTENT BREAKDOWN:

	29	Videos
	21	Readings
	13	Quizzes
	7	Hands-on Exercises
	5	Writing Assignment

Course 2 — Play It Safe: Manage Security Risks

In this course, you'll identify the steps of risk management and explore common threats, risks, and vulnerabilities. Additionally, you'll explore Security Information and Event Management (SIEM) data and use a playbook to respond to identified threats, risks, and vulnerabilities.

By the end of this course, learners will be able to:

- Identify the common threats, risks, and vulnerabilities to business operations.
- Understand the threats, risks, and vulnerabilities that entry-level cybersecurity analysts are most focused on.
- Comprehend the purpose of security frameworks and controls.
- Describe the confidentiality, integrity, and availability (CIA) triad.
- Explain the National Institute of Standards and Technology (NIST) framework.
- Explore and practice conducting a security audit.
- Use a playbook to respond to threats, risks, and vulnerabilities.





SKILLS ACQUIRED:

- ❑ Information Security (INFOSEC)
- ❑ Security Audits
- ❑ Incident Response Playbooks
- ❑ NIST Risk Management Framework
- ❑ NIST Cybersecurity Framework (CSF)

TOPICS:

- ★ Security domains
- ★ Security frameworks and controls
- ★ Introduction to cybersecurity tools
- ★ Use playbooks to respond to incidents

CONTENT BREAKDOWN:

	35	Videos
	20	Readings
	15	Quizzes
	7	Hands-on Exercises

Course 3 — Connect and Protect: Networks and Network Security

In this course, you will explore how networks connect multiple devices and allow them to communicate. You'll start with the fundamentals of modern networking operations and protocols. For example, you'll learn about the Transmission Control Protocol / Internet Protocol (TCP/IP) model and how network hardware, like routers and modems, allow your computer to send and receive information on the internet.

By the end of this course, learners will be able to:

- Describe the structure of different computer networks.
- Illustrate how data is sent and received over a network.
- Recognize common network protocols.
- Identify common network security measures and protocols.
- Explain how to secure a network against intrusion tactics.
- Compare and contrast local networks to cloud computing.
- Explain the different types of system hardening techniques.




SKILLS ACQUIRED:

- ❑ Define the types of networks and components of networks
- ❑ Illustrate how data is sent and received over a network
- ❑ Understand how to secure a network against intrusion tactics
- ❑ Describe system hardening techniques

TOPICS:

- ★ Network architecture
- ★ Network operations
- ★ Secure against network intrusions
- ★ Security hardening

CONTENT BREAKDOWN:

	44	Videos
	31	Readings
	20	Quizzes

Course 4 — Tools of the Trade: Linux and SQL

In this course, you will explore computing skills that you'll use on-the-job as a cybersecurity analyst. First, you'll practice using Linux, an operating system commonly used by cybersecurity professionals.

By the end of this course, learners will be able to:

- Explain the relationship between operating systems, applications, and hardware.
- Compare a graphical user interface to a command line interface.
- Identify the unique features of common Linux distributions.
- Navigate and manage the file system using Linux commands via the Bash shell.
- Use Linux commands via the Bash shell to authenticate and authorize users.
- Describe how a relational database is organized.
- Use SQL to retrieve information from a database.
- Apply filters to SQL queries and use joins to combine multiple tables..





SKILLS ACQUIRED:

- ❑ Linux
- ❑ Command line interface (CLI)
- ❑ Bash
- ❑ SQL

TOPICS:

- ★ Introduction to operating systems
- ★ The Linux operating system
- ★ Linux commands in the Bash
- ★ Databases and SQL

CONTENT BREAKDOWN:

	42	Videos
	34	Readings
	21	Quizzes
	5	Hands-on Exercises

Course 5 — Assets, Threats, and Vulnerabilities

In this course, you will explore the concepts of assets, threats, and vulnerabilities. First, you'll build an understanding of how assets are classified. Next, you will become familiar with common threats and vulnerabilities, and the security controls used by organizations to protect valuable information and mitigate risk. You will develop an attacker mindset by practicing the threat modeling process, and you'll learn tactics for staying ahead of security breaches.

By the end of this course, learners will be able to:

- Learn effective data handling processes.
- Discuss the role of encryption and hashing in securing assets.
- Describe how to effectively use authentication and authorization.
- Explain how common vulnerability exposures are identified by MITRE.
- Analyze an attack surface to find risks and vulnerabilities.
- Identify threats, such as social engineering, malware, and web-based exploits.
- Summarize the threat modeling process.





SKILLS ACQUIRED:

- Vulnerability assessment
- Threat analysis
- Authentication
- Cryptography
- Asset classification

TOPICS:

- ★ Introduction to asset security
- ★ Protect organizational assets
- ★ Vulnerabilities in systems
- ★ Threats to asset security

CONTENT BREAKDOWN:

	43	Videos
	40	Readings
	26	Quizzes
	14	Hands-on Exercises

Course 6 — Sound the Alarm: Detection and Response

In this course, you will focus on incident detection and response. You'll define a security incident and explain the incident response lifecycle, including the roles and responsibilities of incident response teams. You'll analyze and interpret network communications to detect security incidents using packet sniffing tools to capture network traffic.

By the end of this course, learners will be able to:

- Explain the lifecycle of an incident.
- Describe the tools used in documentation, detection, and management of incidents.
- Analyze packets to interpret network communications.
- Perform artifact investigations to analyze and verify security incidents.
- Identify the steps to contain, eradicate, and recover from an incident.
- Determine how to read and analyze logs during incident investigation.
- Interpret the basic syntax and components of signatures and logs in Intrusion Detection Systems (IDS) and Network Intrusion Detection Systems (NIDS) tools.
- Perform queries in Security Information and Event Management (SIEM) tools to investigate an event.






SKILLS ACQUIRED:

- ❑ Security Information and Event Management (SIEM) tools
- ❑ Intrusion Detection Systems (IDS)

TOPICS:

- ★ Introduction to detection and incident response
- ★ Network monitoring and analysis
- ★ Incident investigation and response
- ★ Network traffic and logs using IDS and SIEM tools

CONTENT BREAKDOWN:

	42	Videos
	26	Readings
	20	Quizzes
	10	Hands-on Exercises
	6	Writing Assignment

Course 7 — Automate Cybersecurity Tasks with Python

In this course, you will be introduced to the Python programming language and apply it in a cybersecurity setting to automate tasks. You'll start by focusing on foundational Python programming concepts, including data types, variables, conditional statements, and iterative statements. You'll also learn to work with Python effectively by developing functions, using libraries and modules, and making your code readable. In addition, you'll work with string and list data, and learn how to import, parse and debug files.

By the end of this course, learners will be able to:

- Explain how the Python programming language is used in cybersecurity.
- Write conditional and iterative statements in Python.
- Create new, user-defined Python functions.
- Use Python to work with strings and lists.
- Use regular expressions to extract information from text.
- Use Python to open and read the contents of a file.
- Identify best practices to improve code readability.
- Practice debugging code.






SKILLS ACQUIRED:

- Computer Programming
- Python Programming
- Coding
- PEP 8 style guide

TOPICS:

- ★ Introduction to Python
- ★ Write effective Python code
- ★ Work with strings and lists
- ★ Python in practice

CONTENT BREAKDOWN:

	40	Videos
	32	Readings
	17	Quizzes
	4	Hands-on Exercises
	5	Writing Assignment

Course 8 — Put It to Work: Prepare for Cybersecurity Jobs

In this course, you will focus on making decisions and escalating incidents to stakeholders. You'll develop the communication and collaboration skills needed to inform and influence stakeholders within an organization. In addition, you'll explore how to ethically operate as a cybersecurity professional. You'll discover how to engage with the cybersecurity community, explore jobs in the cybersecurity field, and complete practice interviews. You'll also write a resume and cover letter to prepare for applying and interviewing for jobs in cybersecurity.

By the end of this course, learners will be able to:

- Determine when and how to escalate a security incident.
- Explain how having an ethical mindset supports a cybersecurity professional's ability to protect assets and data.
- Communicate sensitive information with care and confidentiality.
- Use reliable sources to remain current on the latest cybersecurity threats, risks, vulnerabilities, and tools.
- Engage with the cybersecurity community.
- Find and apply for cybersecurity jobs.
- Prepare for job interviews.

SKILLS ACQUIRED:

- Job preparedness
- Stakeholder communication
- Integrity and discretion
- Escalation
- Resume and portfolio preparation

TOPICS:

- ★ Protect data and communicate incidents
- ★ Escalate incidents
- ★ Communicate effectively to stakeholders
- ★ Engage with the cybersecurity community
- ★ Find and apply for cybersecurity jobs

CONTENT BREAKDOWN:



42

Videos



36

Readings



20

Quizzes



4

Hands-on Exercises